Contract Data Processing Schedule (Controller-Processor)

This Contract Data Processing Schedule, including the Data Processing Terms and Conditions and the Description of Processor's Controls (this "DPA"), is attached to and made a part of the Agreement between the User and GHX, acting as data controller and data processor, respectively. The parties agree as follows:

1. Definitions and Data Processing Information

In addition to the terms defined above and elsewhere in the Agreement, capitalized terms used herein will have the meanings defined below. Capitalized terms used but not otherwise defined in this DPA or the Agreement have the meanings defined in the 1995 Directive or, as of May 25, 2018, the GDPR (each as defined below).

Defined Term	Definition
1995 Directive	• Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995
Data Categories	• Contact details; employment details; data concerning health; IT systems information; email content and transmission data; details of goods and services provided; financial details.
Data Subjects	• Past, present, and prospective employees, contractors, suppliers, and agents of the Controller; • Past, present, and future patients of the Controller, and their parents, guardians, and beneficiaries.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
Personal Data	Is as defined in the 1995 Directive or, as of May 25, 2018, the GDPR, and in particular includes personal data that is processed by the Processor on behalf of the Controller.
Processing Activities	Any operation with regard to Personal Data irrespective of the means applied and procedures, in particular obtaining, collecting, recording, organising, storage, holding, use, amendment, adaptation, alteration, disclosure, dissemination or otherwise making available, aligning, combining, retrieval, consultation, testing, archiving, transmission, blocking, erasing, or destruction of Personal Data.
Processing Sites	• Processor offices in Cambridge, United Kingdom; Brussels, Belgium; Dusseldorf and Frankfurt, Germany; Hilversum, The Netherlands; Baar, Switzerland, and Louisville, Colorado, United States; Processor data centers at vendors in the EU/EEA; United Kingdom; Canada; Texas, Virginia, and Washington, United States; and India
Purposes of Processing	• The legitimate interests of the Controller, its suppliers, contractors, and agents, or the Processor in carrying out the Agreement • Preventive or occupational medicine, for the assessment of the working capacity of the data subject, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European Union or member state law or pursuant to contract with a health professional and subject to the conditions and safeguards in the GDPR relating to processing under the responsibility of a professional subject to the obligation of professional secrecy under European Union or member state law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under European Union or member state law or rules established by national competent bodies

Defined Term	Definition
DPA	This Contract Data Processing Schedule, consisting of this cover section and the following incorporated attachments: 1. the Data Processing Terms and Conditions; and 2. the Description of Processor's Controls.
Controller	The User, collectively with its Affiliates and Licensed Facilities, as identified in the Agreement
Processor	The GHX entity identified in the Agreement
Agreement	The agreement(s) for services between the parties or their affiliates, including all addenda, schedules, exhibits, attachments, amendments, and statements of work

Data Processing Terms and Conditions

2. Incorporation into Agreement

The parties agree that this DPA is incorporated into the Agreement effective as of the effective date of the Agreement (the "Effective Date").

3. Data Processing

a. The Processor shall process the Personal Data only on documented instructions from the Controller and in accordance with the Agreement, including with regard to transfers of personal data to a third country or an international organization, unless required to do otherwise by European Union or member state law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

b. The Agreement and this DPA constitute the Controller's general written instructions to process Personal Data, provided that the Controller may issue specific instructions that further restrict such processing so long as in accordance with applicable law.

c. The Processor shall not process the Personal Data for any purpose other than those identified in the cover section of this DPA without the prior analysis and written consent of the Controller.

d. Any rectification, restriction of processing and erasure of Personal Data shall take place only pursuant to the Controller's instructions.

e. If, by virtue of determining the purpose and means of processing any Personal Data, the Processor constitutes a joint controller under the 1995 Directive or GDPR with respect to such Personal Data, the Processor shall comply with provisions of applicable law related to controllers with respect to such Personal Data. In such circumstances, the Controller shall remain the contact point for data subjects.

f. The parties shall comply with applicable law, including without limitation the 1995 Directive and the GDPR, in carrying out this DPA and the Agreement.

g. The Processor shall promptly inform the Controller if, in its opinion, any Controller instruction infringes 1995 Directive, the GDPR, or other European Union or member state data protection provisions.

4. Confidentiality

a. The Processor shall keep Personal Data confidential in accordance with applicable law and the Agreement, using not less than commercially reasonable controls.

b. The Processor shall ensure that persons it authorizes to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. The Processor is aware that the Controller and/or its communication partners are subject to an obligation of secrecy under Union or member state law or rules when exchanging genetic data, biometric data or data concerning health through the Processor's services and acknowledges and agrees that it will also be under such obligation when processing such data.

5. Security

a. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

i. the pseudonymisation and encryption of Personal Data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

b. In assessing the appropriate level of security, the Processor shall in particular take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

c. The Processor may use its documented adherence to an approved code of conduct as referred to in GDPR Article 40 or an approved certification mechanism as referred to in GDPR Article 42 as an element by which to demonstrate compliance with the requirements for technical and organizational measures in this DPA. In such instances, the Processor shall provide the Controller current documentation evidencing such adherence, and shall update its documentation promptly upon any material change in circumstances relating to it.

d. The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process them except on instructions from the Controller, unless he or she is required to do so by European Union or member state law.

e. The Processor has adopted and implemented policies reasonably designed for it to meet the requirements of the 1995 Directive, the GDPR, the Description of Processor's Controls attached to this DPA, and other applicable law (including, where applicable, the German Federal Data Protection Act (*Bundesdatenschutzgesetz*)). The Processor shall provide the Controller copies of such policies upon written request at any time.

6. Subprocessors

a. The Processor shall not engage another data processor of Personal Data without prior specific or general written authorization of the Controller. The parties agree that any provisions of the Agreement expressly permitting engagement of subcontractors will constitute Controller's general written authorization of subprocessing by affiliates of the Processor and by subprocessors providing business process outsourcing, information technology, data hosting and storage, telecommunications, and legal and accounting services. Upon the Controller's written request not more than annually, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors with regular access to more than incidental amounts of Personal Data.

b. Where the Processor engages another data processor for carrying out specific processing activities on behalf of the Controller, the Processor shall enter into a written contract with such other data processor requiring at least the same level of data protection obligations as set out in this DPA, the Agreement, or other legal act between the Controller and the Processor as referred to in this DPA or the GDPR. Such contract must in particular provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this DPA, the 1995 Directive, the GDPR, and/or other applicable laws and, where the other data processor is located in a jurisdiction not providing an adequate level of data protection, ensuring such level of data protection (*e.g.*, Standard Contractual Clauses). The Controller authorizes the Processor to enter into Standard Contractual Clauses with subprocessors in the categories listed above covering transfers of Personal Data to the countries listed under Processing Sites in the cover section of this DPA, and to conduct such transfers without further approval from the Controller. Where that other processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that other processor's obligations.

7. Assistance

a. The Processor shall assist the Controller in ensuring compliance with the obligations pursuant to GDPR Articles 32 through 36, taking into account the nature of processing and the information available to the Processor.

b. Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the individual data subject's rights laid down in the GDPR. The Processor shall promptly forward to the Controller any request of an individual data subject related to Personal Data.

c. The Processor shall assist the Controller with any Data Protection Impact Assessments and consultations and communications with supervisory authorities under the GDPR.

8. Personal Data Breach

a. The Processor shall notify the Controller without undue delay after having become aware of a Personal Data Breach.

b. The Processor's notice of a Personal Data Breach shall at minimum:

i. describe the nature of the Personal Data Breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

ii. communicate the name and contact details of the Processor's data protection officer or other contact point where more information can be obtained;

iii. describe the likely consequences of the Personal Data Breach; and

iv. describe the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

c. Where, and in so far as, it is not possible to provide the required information at the same time, the information may be provided in phases without undue further delay.

d. The Processor shall assist the Controller in documenting and responding to any Personal Data Breach, including without limitation with respect to any communications with the data subjects pursuant to GDPR Article 34.

9. Deletion or Return of Personal Data

a. At the choice of the Controller, the Processor shall delete or return all the Personal Data to the Controller after the end of the provision of services relating to processing, delete existing copies, and safely erase or dispose of all data media as well as all testing and waste materials containing such copies.

b. Notwithstanding the foregoing, the Processor may, so long as it continues to protect the Personal Data in accordance with the standards of applicable law and this DPA:

i. retain such reasonable copies of the Personal Data as as necessary to comply with applicable legal, regulatory, judicial, audit or internal compliance requirements;

ii. retain Personal Data to the extent and so long as required by applicable law; and

iii. retain Personal Data to the extent and so long as it cannot reasonably and practicably be expunged from its systems (for example in automatic backups, latent data, metadata, and data wholly, partially, or jointly owned by other entities).

c. If the Processor retains any Personal Data after expiration or termination of this DPA, the Processor shall promptly delete or return all such Personal Data as soon as the conditions requiring retention permit. The provisions of this DPA will continue to apply to any Personal Data so retained for as long as it is so retained.

d. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of this DPA will be borne by the Controller.

10. Audits and Inspections

a. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the 1995 Directive, the GDPR, and this DPA and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

b. The parties agree that, for any year in which the Processor does not cause a Personal Data Breach, the Processor may meet the above requirements for information by providing the Controller a copy of its current report of a third-party auditor of the Processor's operational controls.

c. Any audit or inspection by or on behalf of the Controller will be limited to information directly relevant to compliance with this DPA and will be conducted after reasonable prior written notice, during regular business hours, and within the Processor's operational, security, and confidentiality requirements.

d. Any third-party auditor selected by the Controller must agree to a confidentiality agreement with the Processor prior to accessing the Processor's information or facilities.

11. Term

The term of this DPA and of the processing begins the Effective Date and continues through expiration or termination of the Agreement.

12. Termination

Either party may terminate this DPA and initiate the termination provisions of the Agreement for cause if the other party materially breaches any provision of this DPA or materially violates applicable provisions of the 1995 Directive, the GDPR, or European Union or member state data privacy law.

13. Survival

The sections of this DPA titled "Confidentiality," "Assistance," "Deletion or Return of Personal Data," "Governing Law," "Severability," and "Non-Waiver," as well as any other provision that, in order to give proper effect to its intent, should survive expiration or termination of this Agreement, will survive such expiration or termination.

14. Notices

All legal notices given under this DPA must be in writing and delivered as provided in the Agreement. A copy of each legal notice must be addressed to the receiving party's General Counsel.

15. Governing Law

a. The 1995 Directive will govern all matters arising out of or relating to this DPA until May 25, 2018, as of which date the GDPR will govern such matters.

b. Notwithstanding the foregoing, where the 1995 Directive or the GDPR permits the application of laws other than the 1995 Directive, the GDPR, other European Union law, or member state law, governing law, jurisdiction, and venue will be as provided in the Agreement.

16. Entire Agreement

This DPA and the Agreement contain the entire agreement between the parties with respect to the subject matter contained herein and supersede all prior negotiations, agreements, and understandings between the parties, whether written or oral, with respect to such subject matter. In the event of a conflict between the terms or conditions of this DPA and the Agreement, the terms of this DPA will take precedence over the conflicting term or condition of the Agreement. This DPA may be amended only by a writing signed by both parties.

17. Severability

If any term or provision in this DPA is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability will not affect any other term or provision of this DPA or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon determination by a court of competent jurisdiction that any term or provision of this DPA is invalid, illegal, or unenforceable, the court may modify this DPA to effect compliance with applicable law and the original intent of the parties as closely as possible.

18. Headings

The headings in this DPA are for convenience only and are not intended to be part of or affect the interpretation of this DPA.

19. Non-Waiver

The waiver by a party of a breach of any provision of this DPA will not operate or be construed as a waiver by such party of any subsequent breach.

Description of Processor's Controls

The Processor shall maintain and update its technical and organizational measures to meet or exceed the requirements described below and of applicable law.

1. **Unauthorized Access**: The Processor maintains the following measures to prevent unauthorized persons from gaining access to data processing systems with which Personal Data are processed or used:

The Processor maintains controls for user access management, system and application access management, physical and environmental security controls, and organizational roles, responsibilities and authorities. The Processor performs risk assessments and monitoring, analysis and evaluation on a recurring basis. The Processor provides training to members of the workforce on initial hire and annually and maintains policy and procedure documents to provide guidance related to unauthorized access.

2. **Unauthorized Use**: The Processor maintains the following measures to prevent data processing systems from being used without authorization:

The Processor maintains controls for user access management, system and application access management, cryptographic controls, physical and environmental security controls, organizational roles, responsibilities and authorities. The Processor performs risk assessments and monitoring, analysis and evaluation on a recurring basis. The Processor provides training to members of the workforce on initial hire and annually and maintains policy and procedure documents to provide guidance related to unauthorized use.

3. **Limited Rights**: The Processor maintains the following measures to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage (access control):

The Processor has implemented controls for user registration and deregistration, role-based user access provisioning, management of privileged access rights, review of user access rights, and removal or adjustment of access rights when roles change. The Processor performs risk assessments and monitoring, analysis and evaluation on a recurring basis. The Processor's workforce training includes guidance related to limited rights.

4. **Transmission**: The Processor maintains the following measures to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged:

To maintain secure data transmission, the Processor employs Secure Hypertext Transfer Protocol (HTTPS), File Transfer Protocol Secure (FTPS), and Virtual Private Network (VPN) protection for standard transmissions of personal data within its products and services. These methods require user ids and passwords, and in some instances multi-factor authentication. The Processor utilizes encryption meeting the standards of the US National Institute of Standards and Technology (NIST) as appropriate. The Processor performs risk assessments and monitoring, analysis and evaluation on a recurring basis.

5. **Audit Trail**: The Processor maintains the following measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems, modified or removed:

Audit trails are maintained by the Processor to log critical events for its key IT infrastructure components and applications. The Processor also maintains a variety of security software to include: (1) remote access software; (2) web proxies; and (3) authentication servers that are a source of computer security log data. The Processor uses logs for recording the actions of users and providing data useful for investigating malicious activity.

6. **Subcontractors**: The Processor maintains the following measures to ensure that, in the case of subcontracted processing of Personal Data, the data are processed strictly in accordance with the instructions of the Controller:

The Processor maintains written agreements with its subcontractors specifying the services to be provided, and maintaining controls over the processing of personal data, including requirements for compliance with instructions. Where appropriate, the Processor enters into data processing agreements and standard contractual clauses with subprocessors. The Processor performs risk assessments and monitoring, analysis and evaluation of subcontractors on a recurring basis. The Processor provides guidance related to the management of subcontractors in its policies and procedures.

7. **Availability**: The Processor maintains the following measures to ensure that Personal Data are protected from accidental destruction or loss:

The Processor utilizes information processing facilities implemented with redundancy for high availability. The Processor monitors and tunes its processing operations, and makes projections of future capacity requirements to maintain system performance. The Processor maintains procedures for backup and restoration, change management, business continuity and disaster recovery, data disposal and media sanitization, and security and privacy incident response. The Processor performs risk assessments and monitoring, analysis and evaluation of availability on a recurring basis.

8. **Separate Processing**: The Processor maintains the following measures to ensure that data collected for different purposes can be processed separately:

Separate processing is maintained by the Processor using the technical capabilities of the deployed software (for example: multi-tenancy or separate system landscapes) to achieve data separation between customers. Appropriate procedures and measures are in place to limit the processing of collected data to the uses permitted under customer agreements, and to provide for separated data processing. The Processor performs risk assessments and monitoring, analysis and evaluation of separate processing on a recurring basis.